OBS Business School

RED DE EDUCACIÓN SUPERIOR
Planeta Formación y Universidades

Jose Alberto Gordo Bravo

Criptografía, sistemas de encriptación y protección y biometría

Actividad 1

Título

Actividad 1: Retos criptográficos.

Objetivo

Tiene como objetivo el establecer las bases de funcionamiento de los algoritmos criptográficos a bajo nivel.

Enunciado

En esta actividad proponemos la resolución de ciertos algoritmos criptográficos. Se darán los datos de entrada en codificación hexadecimal y la clave, en la misma codificación, y el alumno tendrá que calcular el resultado y establecerlo en la casilla "Resultado".

Los algoritmos que se utilizarán son:

HASH:

- SHA1
- SHA256
- SHA512

CIFRADO SIMETRICO:

- 3DES
- AES

FIRMA

- HMACSHA256
- RSA

CIFRADO ASIMETRICO

RSA

DESCIFRADO ASIMETRICO

En el encabezado de cada operación se podrá encontrar el nombre del algoritmo, así como el modo de funcionamiento. Por ejemplo, **AES MODO CBC PKCS PADDING**, es un cifrado AES en modo CBC y aplicando un "padding PKCS" a los datos de entrada.

Tanto las entradas como las claves estarán representadas en codificación Hexadecimal.

Muy importante: La actividad deberá ser presentada a tiempo y subida a la plataforma en formato PDF. En caso de no presentarse en plazo se aplicarán los criterios de la política de penalización que aparece en la guía de la asignatura (siempre y cuando aplicara y se autorizara la entrega tardía: Si no se autoriza por escrito, y se entrega tarde NO será corregido).

Recursos a consultar

- Para resolverlo se dispone de la herramienta **cyberchef** que está disponible en el siguiente link: https://toolbox.itsec.tamu.edu/
- **Recursos obligatorios -> Semana 1.**
- Tenéis ejemplos en la parte de **Recursos voluntarios -> Semana 1**
- Webinar 1.

Calificaciones y Evaluación

Esta actividad corresponde a un 5% de la nota final.

Cada reto o pregunta vale 0,5 puntos en total. La suma de todos es 10 puntos.

Operaciones HASH

HASH SHA1 (0,5 puntos)

INPUT: 12345678

OUTPUT	9bce73d0c8b9eca4f24154f3bd3b8aa473b1c3a9

HASH SHA1 (0,5 puntos)

INPUT: 12121212123434343434565656565656787878

OUTPUT	dc5c7f055956daf0f881ace72e94fbdef6301f32

HASH SHA256 (0,5 puntos)

INPUT: 12345678

OUTPUT	b2ed992186a5cb19f6668aade821f502c1d00970dfd0e35128d51bac4649916c

HASH SHA256 (0,5 puntos)

INPUT: 12121212123434343434565656565656787878

OUTPUT	54a4e64aa24d097a96b776447be6a0518d3444ebc7e385f39aa6b1558c918867

Operaciones Cifrado Simétrico

3DES MODO ECB (0,5puntos)

KEY: 54D65B9D56BB406A6EC77CDFC8FD2E2C1AF4B6B00FF3CE76

INPUT:

21B5C8A9F23295B88A3049A41EA1DD4D39520DB3DE79EB62A83A46F01E1EE5B4

OUTPUT	437683e08a023691178df6d1f283d43fd0d4da4a4201f126a7bc2570d8020e5b

3DES MODO CBC (0,5puntos)

KEY: 54D65B9D56BB406A6EC77CDFC8FD2E2C1AF4B6B00FF3CE76

IV: 1234567890ABCDEF

INPUT:

21B5C8A9F23295B88A3049A41EA1DD4D39520DB3DE79EB62A83A46F01E1EE5B4

OUTPUT	e4136a67d2090f63c4d47121660bb2b98f96af3cccd10cad4b276616f5d81f66

AES MODO CBC (0,5puntos)

KEY:

055A76508042E70345B86E668D793F3656B266D2B55335C7551F667D78C756C2

IV: 1234567890ABCDEF1234567890ABCDEF

INPUT:

21B5C8A9F23295B88A3049A41EA1DD4D39520DB3DE79EB62A83A46F01E1EE5B4

OUTPUT	4168b45f2dc8c9ca855358f5c96e3e2ff5a39cca84a9ae3f632f69080498fbee

AES MODO CBC PKCS PADDING (0,5puntos)

KEY:

055A76508042E70345B86E668D793F3656B266D2B55335C7551F667D78C756C2

IV: 01910191817161710191019181716171

INPUT:

21B5C8A9F23295B88A3049A41EA1DD4D39520DB3DE79EB62A83A46F01E1EE5B4

OUTPUT	432938d20977d7e34d0726683a60dbea93d495ac2a471779f7a3e25d58a7d1c6724be0facff6eb0d9691864860aab6bd

AES MODO GCM (0,5puntos)

KEY:

055A76508042E70345B86E668D793F3656B266D2B55335C7551F667D78C756C2

IV: 01910191817161710191019181716171

INPUT:

21B5C8A9F23295B88A3049A41EA1DD4D39520DB3DE79EB62A83A46F01E1EE5B4

OUTPUT	84c375750517e7c4827e98925e72c5558cb54f9ff2aa3e83aeebe9fb79c1fb8eb1f8a9ed49e297d016b1d502348b8375

PREGUNTAS

¿Sabrías explicar cómo se realiza un padding PKCS? (0,5puntos)

RESUESTA	Se completa el bloque con bytes cuyo valor es el número de bytes añadidos. En AES, si faltan 5 bytes, se agregan 05 05 05 05 05.

¿Sabrías explicar qué pasaría si cifrados con AES-ECB o AES-CBC una cantidad de información cuya longitud no es múltiplo de 16 bytes? (0,5puntos)

RESUESTA	Sin padding no se puede cifrar correctamente el último bloque; hay que completar hasta 16 bytes.

¿Sabrías comentar qué diferencias observas entre el AES-GCM y el resto de algoritmos simétricos que has probado en este ejercicio? (0,5puntos)

RESUESTA	AES-GCM además de cifrar genera autenticación e integridad con un tag.

Operaciones FIRMA Simétrica

HMAC-SHA256 (0,5puntos)

KEY: 54D65B9D56BB406A6EC77CDFC8FD2E2C1AF4B6B00FF3CE76

INPUT: 1234567890ABCDEF

OUTPUT	ef2a6a582be51faa2c6a5306810b5338b845be43ad2cac5e628b10b451f9e3dd

HMAC-SHA256 (0,5puntos)

KEY: 54D65B9D56BB406A6EC77CDFC8FD2E2C1AF4B6B00FF3CE76

INPUT: 1234567890ABCDFF

OUTPUT	85e2cfc87991c40ddad9f77bbbaf4b7f681ee5da488d40db6d12a633086108a2

Operaciones FIRMA Asimétrica

FIRMA RSA-PKCS1 v1.5 SHA256 (0,5puntos)

PRIVATEKEY:

-----BEGIN RSA PRIVATE KEY-----

MIICXAIBAAKBgQCykkdR+9PBkKydz0b/xqk2yixztv0ntyrOXdMO1zM6dYHSYc1R

zloEqioA0//+9BlElnDB8VYr8MImTS1HGIOtawd95ZfCocbUrmdoKDEbeBkoofD8

kgPpmA6PKYNe2YImNl7dYvS51xvVSxJEN9nif9frZAqf3nXi7rd6oXtZiwIDAQAB

AoGARZvl91xuOFc4IrApIg2D6tq2p0jeuDubkSRb4L4ctx4VRDhhvBDvYEAg7X+2

m+D1dJocTE3SZICOfjW5f6xbr3fs8Y8UfGartyPvXDq7BkISr8MuTc8T2Skmtj1/

29vn89UbN1R7nxlBqtWGTit3rHRdBB75L55No8baQaEEv0kCQQDoxGysMj2ADIGU

0930csHNW7ggEaXH5CJARn7jxmXvWpv7IjrO8ccFgZ9s0dVyzfMGN83Ay4VOw8Bh

Xr20QrVfAkEAxGUQFOP6H1TqoxsmIlCfimdSpZXv6amxG1uQpWUtTjQWq+tuvm4I

zjUrmuF9O1+Hf90Y4MAx8eBj0oT+q4V/VQJBAOPymEn52Whw1uWcphwh1dD6JVKi

datPqosvfkwpmuHP5jkFyHmpJLIrwqiaxWFsdrZ8J67KoH4GDXxNf5HsUhkCQCrA

PSHvBnFvkKv0qvZpSnFcUHdPDix1DeKAqhn2zkfpus2tsCuv1CbfGCDc2N/lyZ8h

x9qUu8qFJ/WZkb5QjwkCQGnfAYmq/IQWSdWm9hcAlrt6Ne7dNf09QjD8i8YwdfNi

3QBa+PqLF+7gEIX20cWWf9Eb3IxRoqf/5s3yPsCZ9tk=

-----END RSA PRIVATE KEY-----

INPUT: 1234567890ABCDEF

OUTPUT	

6cf5d4d84f183e7e6937ba9b7c71875bc19144dd1a9025fe0d7ffe36c77a0ce42ae3f23b30074cfa42afb3971c9e51876
6d30bab2d6cfe3df4d730571b596b8756e4efe11fa76be1dfc01db7b9f8cfea5c23eb5f5c12bcf80afe31c134066af27efb
21615c597a6de25be4ee9cdd22b9ad3df75d3213d9a9dec921bbfbe01185

Operaciones Cifrado Asimétrico

CIFRADO - RSAPKCS1 v1.5 (0,5puntos)

PUBLICKEY:

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm4bPyM/s0o+ftmmQNzlF
CYCs17A0ZVbgyxiGpLqfVeIKv41gZzDCZ75c2ox6NIiRHgMHATW9hwMJ+sjhTHzD
p6nVlskwYdRSbJCwmR1BqiJfRC8hsgmIcNh1i7JyerPE1pXKkBuFFiMGgII3pKye
9l5g/v2qFEAyrJyc9e0YXhhnW3D/93xTBOa923XRygG5Nelk1d1BO/BzVsu5Y15z
Bn23XwtuF0y5t9uLi329V8XywM/dM5T7ubod/k2LOLKvuHerqmBIVQWQEPeVdIO1
FinGoUn+AEfrQo4InPMw+haez2v+bcmH0WBlx+BQwV4FrvCN0fb5fsGYGbG6nwoG
qwIDAQAB

-----END PUBLIC KEY-----

INPUT: 1234567890ABCDEF

OUTPUT	7c1a7dbbbc608b6e8fd52618a91ad78f9f75f2b4d0b47cb60b39da1f237ad437ea63af1a8bc05d557436ece1dee4c7895cc6577d7b75a228e1766b6091b648dcd2eda63e6ac8210a551e4c83cd1f034dcf7f3959e00ce29a229c1ed488548ef27f9d2b3cf2667bd40f8daa40c8929c16b58469170096ee51c59f5b2f2e51755d8d47dea9267b52834648dd1247d5ca7fcc6b0b7d13e8b2214879133572942a5151ded7e8d21932cc3eeb81e7d041953684bb231be15700895e4afe670262db4f5fab284a4d4c05a49ec699848c862b6b7757989435adab657ed53af0b8a79097fb5c2bdaab57b0a8cc0d3920ca5092b48aa4c580e792168cd4e6f667c3dc967c

CIFRADO - RSAPKCS1 v1.5 (0,5puntos)

PUBLICKEY:

-----BEGIN PUBLIC KEY-----

MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAm4bPyM/s0o+ftmmQNzlF
CYCs17A0ZVbgyxiGpLqfVeIKv41gZzDCZ75c2ox6NIiRHgMHATW9hwMJ+sjhTHzD
p6nVlskwYdRSbJCwmR1BqiJfRC8hsgmIcNh1i7JyerPE1pXKkBuFFiMGgII3pKye
9l5g/v2qFEAyrJyc9e0YXhhnW3D/93xTBOa923XRygG5Nelk1d1BO/BzVsu5Y15z
Bn23XwtuF0y5t9uLi329V8XywM/dM5T7ubod/k2LOLKvuHerqmBIVQWQEPeVdIO1
FinGoUn+AEfrQo4InPMw+haez2v+bcmH0WBlx+BQwV4FrvCN0fb5fsGYGbG6nwoG
qwIDAQAB

-----END PUBLIC KEY-----

INPUT: 1234567890ABCDEF

OUTPUT	810913e25f6f8951c129e3b44b3b9292d79aed0a1b9e344119355abff2fa2ae0dd010e637d718db19683c7f6790d40ffd3f1693a4361355a5764b60d2fe0ff687b8ae530fc58202a858846f45e51617e02c2f2d98fb50b6fe422f1580df46c876bd4b4c33e49998e9e95e3f7cbf6f4262894a8e294a77d4f801c92807eeaa878364148b7254afadbf46ba8623c18ce2780f4885eacd89b3c82c29c581c71bbd19ffcae5b6e9ec17817ac64b4398d0e20142fb59bdb4e00e598e270d4f72f3b8ccd60e1900acd096ce1cf20f7814fe2ade75d5ccc3a9900d8a2fa509ee57504f8638d88cc301ceb24c6fa55b8af781fc1ebb8a9ba46d7434d84217cc6f8f9a125

PREGUNTAS

¿Qué observas en esta operación? (0,5puntos)

RESUESTA	Que cifrando el mismo mensaje con la misma clave pública salen resultados distintos.

¿Sabrías explicar por qué ocurre esto? (0,5puntos)

RESPUESTA	Porque RSA PKCS#1 v1.5 usa padding aleatorio antes del cifrado.

Operaciones Descifrado Asimétrico

DESCIFRADO - RSAPKCS1 v1.5 (0,5puntos)

PRIVATEKEY:

-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAm4bPyM/s0o+ftmmQNzlFCYCs17A0ZVbgyxiGpLqfVeIKv41g
ZzDCZ75c2ox6NIiRHgMHATW9hwMJ+sjhTHzDp6nVlskwYdRSbJCwmR1BqiJfRC8h
sgmIcNh1i7JyerPE1pXKkBuFFiMGgII3pKye9l5g/v2qFEAyrJyc9e0YXhhnW3D/
93xTBOa923XRygG5Nelk1d1BO/BzVsu5Y15zBn23XwtuF0y5t9uLi329V8XywM/d
M5T7ubod/k2LOLKvuHerqmBIVQWQEPeVdIO1FinGoUn+AEfrQo4InPMw+haez2v+
bcmH0WBlx+BQwV4FrvCN0fb5fsGYGbG6nwoGqwIDAQABAoIBADedJnINgAbvWtI0
v2Av93Llc2kRVjsirPGTDJqdLVrdoLBMkrtzoSDN3pA8CXr9lr7foEKbf/Fmccwe
xwm914z92yW3PbjN3sd5mdy2rIN1FRHhtK/gXszTan0Qy4T7AZkmKTAM1zNKRQnx
Boq5O4KnzxF/jbD+H+C/hBUgukTy8EgOmup6YE0e04Ne7lKxEZBHWQJbBbxP+q/A
aLMZGLVzsP/RzMrqwLiTOAjVoFBmNp7mpMdK3i0dZxbtJu7ChYVD8nK3RgEihaB2
FwxmC7O/qryvs0Yf66EokQIzrutsyjCl0vm9U+/jAU3JnIyJwG89y6XultBrRywT
yGeTFkECgYEAzTLfPhlRrD9crvaMwcWvXsMITdkOBQnhiIS7bVVAA8sbLbSVIxzC
HOSTc86mMzxJwSBUjfMF7ImxgtDzny6ObwwnCleLXgnhcUN3arpvXcCwbbBJUb2F
6M75H14S+MA5SXiywzgqt50oABOKeGXG+bXKA6gcot2A0eBcwllELeECgYEAwgfP
XjV0rHq4d3R3b6uKGEeAbr3ufLrZf+8N8YuwyH7bZ6/qTudG2yRnE7TIq6d34PQA
ndmP1zmbhL827HHbwk780JKkDlOn60DcAkgQ/1KkBYMjCin4NJSBBFmkgjZDTPSV
bVUv2kBmqFpeGZJISUciHeOyi6/V2GtPFmhRzgsCgYEAiMUZq2hw2aA6BJxs4VME
OuNAC7Na9tzJKJdf3dXunxineuVcalTmxR9NcOkSOiA7ALCt6xdKoYh9erYPS9Ba
O4YcF3aWfA2V6EqRs9+kDxc6AUJ4/DSYpr4dqlynxIlLJb9/V0N+pXfoi3R63Rjp
cNNMXPeWbq+5ByrGaPvax8ECgYBvYPRUa/MRn1CMobp9y8Z1sXW0HCruRoPbwGoM
oddVAB0KJB0oNfKikP7qfPhEMNnLs8U211COh28SgIESsTkpDRZq1AKAhtz5Wj3w
wVWgetvUnjZa+0STSjvVN3ALnwJ7BltQa3oQmq9TLKyfmS0Ng1u+NJqlPMZQeSjo
//EViQKBgGCqUbUOv063MPzotPPJdiQFutjSg0in7C+aHzEjRyG9NX0s7RxJ3oUX
A58Tm8qY4sEWwCSgpik6d7FRwJUil4Tg6hJ0x6w6j10YFzP47wSSKpHbE4IFseoO
RVOkWphKtTI5WrCFz5kizVlK0kvI43R6BsPSilE+5wYA684DtnF5
-----END RSA PRIVATE KEY-----

INPUT: **OUTPUT ANTERIOR CASO**

OUTPUT	1234567890ABCDEF